REMARKS

This is a full and timely response to the final Office Action of July 23, 2004. Reexamination, reconsideration, and allowance of the application and all presently pending claims are respectfully requested.

Upon entry of this First Response, claims 1-17 and 19-36 are pending in this application, and claims 1-17 and 19-30 presently stand rejected.

Response to §103 Rejections

In order for a claim to be properly rejected under 35 U.S.C. §103, the combined teachings of the prior art references must suggest all features of the claimed invention to one of ordinary skill in the art. See, *e.g.*, *In Re Dow Chemical*, 5 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1988), and *In re Keller*, 208 U.S.P.Q. 871, 881 (C.C.P.A. 1981). In addition, "(t)he PTO has the burden under section 103 to establish a *prima facie* case of obviousness." *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988) (Citations omitted). Furthermore, the Federal Circuit has stated that "(i)t is impermissible, however, to simply engage in hindsight reconstruction of the claimed invention, using the applicant's structure as a template and selecting elements from references to fill the gaps." *In re Gorman*, 933 F.2d 982, 987, 18 U.S.P.Q.2d 1885 (1991).

Claim 1

Claim 1 presently stands rejected under 35 U.S.C. §103 as allegedly unpatentable over *Kaplan*. Claim 1 reads as follows:

> 1. A system for securely transmitting data messages, comprising:
>
> a first computer configured to transmit a data message, said data message having a header and a data portion, said first computer configured to encrypt said data portion via a first encryption technique and to encrypt said header via a second encryption technique, said first computer further configured to include information associated with said first encryption technique in said header; and
>
> ***a second computer configured to receive said first data message and to decrypt said header, said second computer further configured to decrypt said data portion based on said information included in said header.***
>
> (Emphasis added).

Applicant respectfully submits that *Kaplan* fails to teach or suggest the features of claim 1 highlighted hereinabove.

Specifically, the Office Action states that

> "[i]t is obvious that the RCC and the producer can be software run on the same computer and providing the cryptolope to the user. Therefore, the second computer would be made up of the producer and the RCC. The role of the RCC is purely administrative. The first computer would be the UPC, which is the consumer of the cryptolope."

See Office Action at page 2.

Albeit, Applicant agrees with the Office Action conclusion that *Kaplan* "does not expressly disclose a system consisting of two computers." See Office Action at page 3. However, even if, as suggested by the Office Action, the Publisher and the Royalty Clearing Center (RCC) are merged into a single computer, *Kaplan* still fails to teach or suggest "a second computer configured to receive said first data message and to decrypt said header, said second computer further configured

to decrypt said data portion based on said information included in said header," as claimed in claim 1.

In this regard, even if the merged computer can "carry out the functionality of the Publisher and the Royalty Clearing Center," which the Office Action concludes is "key distribution and the encryption of data," there is nothing in the cited art to indicate that a second computer, i.e., the user's personal computer (UPC), receives the cryptolope, decrypts the header, and uses the decrypted header to decrypt the data.

To the contrary, the UPC transmits encrypted "key records," which do not appear to contain information sufficient to decrypt the data portion of the cryptolope, to the Royalty Clearing Center (RCC). See *Kaplan*, page 7, *"Buying" a Cryptolope*, paragraph 1. Upon receipt, "[t]he RCC 'translates' the document keys of the cryptolope by decrypting the key records using its private master key(s) and re-encrypting the document keys under [a] public key." See *Kaplan*, page 7, *"Buying" a Cryptolope*, paragraph 5. "The RCC 'Packages' the translated, encrypted document keys...into a license cryptolope which will be processed by the user's cryptolope viewer 'plug-in' software," and the RCC transmits the "license cryptolope" back to the UPC. See *Kaplan*, page 7, *"Buying" a Cryptolope*, paragraph 7. Thus, the RCC, not the UPC, decrypts the header received in the data message.

Accordingly, it does not appear that *Kaplan* discloses "a second computer" configured to decrypt both a "data portion" ***and*** a "header" of the same "data message," as claimed in claim 1. Therefore, Applicant respectfully traverses the Office Action assertion that *Kaplan* suggests or teaches each feature of pending claim 1 and requests that the §103 rejection of claim 1 be withdrawn.

Claims 2-10 and 25-29

Claims 2-4 and 25-29 presently stand rejected in the Office Action under 35 U.S.C. §103 as allegedly unpatentable over *Kaplan,* and claims 5, 7, and 8 presently stand rejected under 35 U.S.C. §103(a) over *Kaplan* in view of *Xiao.* Further, claim 6 presently stands rejected under 35 U.S.C. §103(a) over *Kaplan* in view of *Xiao* and in further view of *Schneier*, and claim 9 presently stands rejected under 35 U.S.C. §103(a) over *Kaplan* in view of *Leppek.* Applicant submits that pending dependent claims 2-10 and 25-29 contain all features of their respective independent claim 1. Since claim 1 should be allowed, as argued hereinabove, pending dependent claims 2-10 and 25-29 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988). Furthermore, these dependent claims recite patentably distinct features and/or combinations of features that make them allowable, notwithstanding the allowability of their base claim 1.

For example, claim 2 reads as follows:

> 2. The system of claim 1, wherein said information associated with said first encryption technique identifies said second encryption technique.

Applicant respectfully asserts that the cited art fails to suggest at least the features of claim 2 recited hereinabove.

In this regard, *Kaplan* teaches that the RCC decrypts key records received from the UPC using a master key(s) that is stored on the RCC. See *Kaplan*, page 7, *"Buying" a Cryptolope*, paragraph 5. The RCC re-encrypts the key records using a public key associated with the UPC, and transmits the re-encrypted key records to the UPC. See *Kaplan*, page 7, *"Buying" a Cryptolope*, paragraph 7. However, *Kaplan* does not teach "information associated with said first encryption technique identifies said second encryption technique," as claimed in claim 2.

Claim 11

Claim 11 presently stands rejected under 35 U.S.C. §103 as allegedly unpatentable over *Kaplan*. Claim 11 reads as follows:

> 11. A system for transmitting messages, comprising:
> means for defining a data portion of a data message;
> means for encrypting said data portion via a first encryption technique;
> means for defining a header of said data message, said header including information associated with said first encryption technique;
> means for encrypting said header via a second encryption technique;
> means for transmitting said message;
> ***means for receiving said message at a client that is remotely located from said transmitting means;***
> ***means for decrypting said header at said client; and***
> ***means for decrypting said data portion at said client based on said information in said header associated with said first encryption technique.*** (Emphasis added)

Applicant asserts that *Kaplan* fails to teach or suggest at least the features of claim 11 highlighted above for at least those reasons argued with respect to claim 1. Accordingly, Applicant respectfully requests that the §103 rejection of claim 11 be withdrawn.

Claim 12

Claim 12 presently stands rejected under 35 U.S.C. §103 as allegedly unpatentable over *Kaplan*. Claim 12 reads as follows:

> 12. A method for transmitting messages, comprising the steps of:
>
> defining a data portion of a first data message;
>
> encrypting said data portion of said first data message via a first encryption technique;
>
> defining a header of said first data message, said header of said first data message including information associated with said first encryption technique;
>
> encrypting said header of said first data message via a second encryption technique;
>
> transmitting said first data message subsequent to said encrypting steps;
>
> ***receiving said first data message at a client that is remotely located from said transmitting means;***
>
> ***decrypting said header at said client;***
>
> ***decrypting said data portion at said client based on said information in said header associated with said first encryption technique.***

Applicant asserts that *Kaplan* fails to teach or suggest at least the features of claim 12 highlighted above for at least those reasons argued with respect to claim 1. Accordingly, Applicant respectfully requests that the §103 rejection of claim 12 be withdrawn.

Claims 13-24

Claim 13 presently stands rejected under 35 U.S.C. §103 as being unpatentable over *Kaplan* in view of *Leppek*, and claims 14-19 stand rejected under 35 U.S.C. §102 as allegedly unpatentable over *Kaplan*. Further, claim 20 stands rejected under 35 U.S.C. §103 over *Kaplan* in view of *Xiao*, and claim 21 stands rejected under 35 U.S.C. §103 over *Kaplan* in view of *Xiao* and further in view of *Schneier*. Also, claims 22-24 stand rejected under 35 U.S.C. §103 over *Kaplan* in view of *Leppek*. Applicant submits that pending dependent claims 13-24 contain all features of their

respective independent claim 12. Since claim 12 should be allowed, as argued hereinabove, pending dependent claims 13-24 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988). Furthermore, these dependent claims recite patentably distinct features and/or combinations of features that make them allowable, notwithstanding the allowability of their base claim 12.

Claim 30

Claim 30 presently stands rejected under 35 U.S.C. §103 as allegedly unpatentable over *Kaplan*. Claim 30 reads as follows:

> 30. A method for securely communicating data messages, comprising the steps of:
> ***receiving at a client a data packet transmitted from a server that is remotely located from said client, said data packet having a first portion encrypted via a first encryption technique and said data packet having a second portion encrypted via a second encryption technique, said second portion comprising information associated with said first encryption technique;***
> ***decrypting, at said client, said second portion to recover said information; and***
> ***decrypting, at said client, said first portion based on said information***. (Emphasis added).

Applicant asserts that *Kaplan* fails to teach or suggest at least the features of claim 30 highlighted above for at least those reasons argued with respect to claim 1.

Furthermore, however, claim 30 recites additional limitations not taught by *Kaplan*. In this regard, the cryptolope taught in *Kaplan* comprises an "encrypted part(s)" and a "key record," which comprises document key(s) that can be used to decrypt the "encrypted part(s)." However, the document key(s) are encrypted, as well, and *Kaplan* does not teach that the information for decrypting these key(s) are contained in the cryptolope. In order to decrypt the encrypted document

key(s), the key records appear to be transmitted to a ***remote computer*** that houses a master key(s) that is used to decrypt the key records. See *Kaplan*, page 3, paragraph 3; page 7, *"Buying" a Cryptolope*, paragraph 7.

Accordingly it does not appear that *Kaplan* teaches "a second portion encrypted via a second encryption technique, said second portion comprising information associated with said first encryption technique," "decrypting, **at said client**, said second portion to recover said information," "and "decrypting, **at said client**, said first portion based on said information," as described by pending claim 30. (Emphasis added).

For at least the above reasons, Applicant respectfully requests allowance of claim 30 and that the 35 U.S.C. §103 rejection of claim 30 be withdrawn.

Claim 31

Claim 31 presently stands rejected under 35 U.S.C. §103 as allegedly unpatentable over *Kaplan*. Claim 31 reads as follows:

> 31. A system for securely transmitting data messages, comprising:
>
> a first computer configured to transmit a data packet comprising a first and a second portion, said first portion encrypted by a first encryption technique and said second portion encrypted by a second technique, said second portion encrypting a public key for decrypting said first portion;
>
> ***a second computer configured to receive said data packet and decrypt said second portion to generate a public key for decrypting said first portion, said second computer further configured to decrypt said first portion with said public key.*** (Emphasis added).

Applicant asserts that *Kaplan* fails to teach or suggest at least the features of claim 31 highlighted above for at least those reasons argued with respect to claim 1 and claim 30. Accordingly, Applicant respectfully requests allowance of claim 31 in its present form.

Claims 32 and 33

Claims 32 and 33 presently stand rejected under 35 U.S.C. §103 as allegedly unpatentable over *Kaplan*. Applicant submits that pending dependent claims 32 and 34 contain all features of their respective independent claim 31. Since claim 31 should be allowed, as argued hereinabove, pending dependent claims 32 and 33 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

Claim 34

Claim 34 presently stands rejected under 35 U.S.C. §103 as allegedly unpatentable over *Kaplan*. Claim 34 reads as follows:

> 34. A method for securely transmitting data messages, comprising the steps of:
>
> transmitting a data packet comprising a first and a second portion, said first portion encrypted by a first encryption technique and said second portion encrypted by a second technique, said second portion encrypting a public key for decrypting said first portion;
>
> ***receiving said data packet by a computer;***
>
> ***decrypting said second portion by said computer to generate a public key for decrypting said first portion; and***
>
> ***decrypting said first portion by said computer with said public key.*** (Emphasis added).

Applicant asserts that *Kaplan* fails to teach or suggest at least the features of claim 34 highlighted above for at least those reasons argued with respect to claim 1 and 31. Accordingly, Applicant respectfully requests allowance of claim 34 in its present form.

Claims 35 and 36

Claims 35 and 36 presently stand rejected under 35 U.S.C. §103 as allegedly unpatentable over *Kaplan*. Applicant submits that pending dependent claims 35 and 36 contain all features of their respective independent claim 34. Since claim 34 should be allowed, as argued hereinabove, pending dependent claims 35 and 36 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

CONCLUSION

Applicant respectfully requests that all outstanding objections and rejections be withdrawn and that this application and all presently pending claims be allowed to issue. If the Examiner has any questions or comments regarding Applicant's response, the Examiner is encouraged to telephone Applicant's undersigned counsel.

Respectfully submitted,

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.

By: _____

Ann I. Dennen
Reg. No. 44,651
(256) 704-3900 Ext. 101

Thomas, Kayden, Horstemeyer & Risley, LLP
100 Galleria Parkway, Suite 1750
Atlanta, GA 30339-5948